

Translation

Rec'd PCT/PTO 13 MAY 2005

PCT/AT2003/000351

PATENT COOPERATION TREATY

PCT

10/535363

INTERNATIONAL PRELIMINARY REPORT ON PATENTABILITY  
(Chapter II of the Patent Cooperation Treaty)

(PCT Article 36 and Rule 70)

Applicant's or agent's file reference R 42658	FOR FURTHER ACTION See Form PCT/IPEA/416	
International application No. PCT/AT2003/000351	International filing date (day/month/year) 21 November 2003 (21.11.2003)	Priority date (day/month/year) 22 November 2002 (22.11.2002)
International Patent Classification (IPC) or national classification and IPC H04L 9/08		
Applicant ARC SEIBERSDORF RESEARCH GMBH		

<p>1. This report is the international preliminary examination report, established by this International Preliminary Examining Authority under Article 35 and transmitted to the applicant according to Article 36.</p> <p>2. This REPORT consists of a total of <u>5</u> sheets, including this cover sheet.</p> <p>3. This report is also accompanied by ANNEXES, comprising:</p> <p>a. <input checked="" type="checkbox"/> (sent to the applicant and to the International Bureau) a total of <u>2</u> sheets, as follows:</p> <p><input type="checkbox"/> sheets of the description, claims and/or drawings which have been amended and are the basis of this report and/or sheets containing rectifications authorized by this Authority (see Rule 70.16 and Section 607 of the Administrative Instructions).</p> <p><input type="checkbox"/> sheets which supersede earlier sheets, but which this Authority considers contain an amendment that goes beyond the disclosure in the international application as filed, as indicated in item 4 of Box No. I and the Supplemental Box.</p> <p>b. <input type="checkbox"/> (sent to the International Bureau only) a total of (indicate type and number of electronic carrier(s)) _____, containing a sequence listing and/or tables related thereto, in computer readable form only, as indicated in the Supplemental Box Relating to Sequence Listing (see Section 802 of the Administrative Instructions).</p>	
<p>4. This report contains indications relating to the following items:</p> <p><input checked="" type="checkbox"/> Box No. I Basis of the report</p> <p><input type="checkbox"/> Box No. II Priority</p> <p><input type="checkbox"/> Box No. III Non-establishment of opinion with regard to novelty, inventive step and industrial applicability</p> <p><input type="checkbox"/> Box No. IV Lack of unity of invention</p> <p><input checked="" type="checkbox"/> Box No. V Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement</p> <p><input type="checkbox"/> Box No. VI Certain documents cited</p> <p><input type="checkbox"/> Box No. VII Certain defects in the international application</p> <p><input type="checkbox"/> Box No. VIII Certain observations on the international application</p>	

Date of submission of the demand 16 June 2004 (16.06.2004)	Date of completion of this report 16 December 2004 (16.12.2004)
Name and mailing address of the IPEA/EP	Authorized officer
Facsimile No.	Telephone No.

## INTERNATIONAL PRELIMINARY REPORT ON PATENTABILITY

International application No.

PCT/AT2003/000351

## Box No. I Basis of the report

1. With regard to the language, this report is based on the international application in the language in which it was filed, unless otherwise indicated under this item.

- ☐ This report is based on translations from the original language into the following language \_\_\_\_\_, which is language of a translation furnished for the purpose of:
- ☐ international search (under Rules 12.3 and 23.1(b))
  - ☐ publication of the international application (under Rule 12.4)
  - ☐ international preliminary examination (under Rules 55.2 and/or 55.3)

2. With regard to the elements of the international application, this report is based on *(replacement sheets which have been furnished to the receiving Office in response to an invitation under Article 14 are referred to in this report as "originally filed" and are not annexed to this report)*:

- ☐ The international application as originally filed/furnished
- ☒ the description:
- pages \_\_\_\_\_ 1-24 \_\_\_\_\_, as originally filed/furnished
- pages\* \_\_\_\_\_ received by this Authority on \_\_\_\_\_
- pages\* \_\_\_\_\_ received by this Authority on \_\_\_\_\_
- ☒ the claims:
- pages \_\_\_\_\_, as originally filed/furnished
- pages\* \_\_\_\_\_, as amended (together with any statement) under Article 19
- pages\* 6 (part), 7-10 received by this Authority on 19 June 2004 (19.06.2004)
- pages\* 1-5, 6 (part) received by this Authority on 11 November 2004 (11.11.2004)
- ☒ the drawings:
- pages \_\_\_\_\_ 1/11-11/11 \_\_\_\_\_, as originally filed/furnished
- pages\* \_\_\_\_\_ received by this Authority on \_\_\_\_\_
- pages\* \_\_\_\_\_ received by this Authority on \_\_\_\_\_
- ☐ a sequence listing and/or any related table(s) – see Supplemental Box Relating to Sequence Listing.

3. ☐ The amendments have resulted in the cancellation of:

- ☐ the description, pages \_\_\_\_\_
- ☐ the claims, Nos. \_\_\_\_\_
- ☐ the drawings, sheets/figs \_\_\_\_\_
- ☐ the sequence listing (*specify*): \_\_\_\_\_
- ☐ any table(s) related to sequence listing (*specify*): \_\_\_\_\_

4. ☐ This report has been established as if (some of) the amendments annexed to this report and listed below had not been made, since they have been considered to go beyond the disclosure as filed, as indicated in the Supplemental Box (Rule 70.2(c)).

- ☐ the description, pages \_\_\_\_\_
- ☐ the claims, Nos. \_\_\_\_\_
- ☐ the drawings, sheets/figs \_\_\_\_\_
- ☐ the sequence listing (*specify*): \_\_\_\_\_
- ☐ any table(s) related to sequence listing (*specify*): \_\_\_\_\_

\* If item 4 applies, some or all of those sheets may be marked "superseded."

## INTERNATIONAL PRELIMINARY EXAMINATION REPORT

International application No.

PCT/AT 03/00351

## V. Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement

## 1. Statement

Novelty (N)	Claims	1-10	YES
	Claims		NO
Inventive step (IS)	Claims	1-10	YES
	Claims		NO
Industrial applicability (IA)	Claims	1-10	YES
	Claims		NO

## 2. Citations and explanations

This report makes reference to the following document:

D1: ELLIOTT C: "Building the quantum network" NEW JOURNAL OF PHYSICS, 2002, DEUTSCHE PHYSIKALISCHE GESELLSCHAFT & IOP PUBLISHING LTD, UK, vol. 4, 12 July 2002 (2002-07-12), pages 46.1-46.12, XP002271991 ISSN: 1367-2630

1. D1, which is considered to represent the prior art closest to the subject matter of claim 1, discloses a communication system using quantum cryptography (page 46.8, lines 15-26) and comprising end switching stations (figure 5, "QKD Endpoint") connected to quantum channels, quantum cryptographic devices assigned to the quantum channels for the purpose of generating a quantum key (page 46.9, lines 5-6) and multiple interconnected switching stations (figure 5, "Trusted Relay"), wherein the switching stations communicate with each other over public lines using specified coding (figure 5, upper white arrows and page 46.9, lines 20-24) and the end switching stations are connected to the switching stations via the quantum channels for the purpose of

generating a temporary quantum key and in addition for communication over public lines using the quantum key generated via the switching stations (page 46.9, lines 20-24).

- 1.1 The subject matter of claim 1 thus differs from the known communication system in that the *subscriber stations* are connected *directly* to the quantum channels and in that the switching stations communicate with each other over public lines using specified coding *without quantum cryptographic key exchange*.

The subject matter of claim 1 is therefore novel (PCT Article 33(2)).

- 1.2 The problem addressed by the present invention may therefore be considered that of (1) extending the high level of security ensured by quantum cryptography to the end user and (2) configuring the overall system in a more economical manner by reducing the number of switching stations.

The solution proposed in claim 1 of the present application involves an inventive step (PCT Article 33(3)). The reasons are:

D1 does not mention the objective of extending the especially secure communication ensured by quantum cryptography to the end user. Although D1 addresses the high cost of switching stations, it does not suggest more economic configuration of the overall system by providing that the switching stations communicate with each other over public lines using specified coding without quantum cryptographic key

INTERNATIONAL PRELIMINARY EXAMINATION REPORT

International application No.

PCT/AT 03/00351

exchange.

2. Claims 2-10 are dependent on claim 1 and therefore likewise meet the PCT requirements for novelty and independent step.

# VERTRAG ÜBER DIE INTERNATIONALE ZUSAMMENARBEIT AUF DEM GEBIET DES PATENTWESEN

## PCT

Rec'd PCT/10

REC'D 16 DEC 2004  
18 MAY 2005  
WIPO PCT

## INTERNATIONALER VORLÄUFIGER PRÜFUNGSBERICHT (Artikel 36 und Regel 70 PCT)

10/535363



Aktenzeichen des Anmelders oder Anwalts R 42658	<b>WEITERES VORGEHEN</b> siehe Mitteilung über die Übersendung des internationalen vorläufigen Prüfungsberichts (Formblatt PCT/PEA/416)	
Internationales Aktenzeichen PCT/AT 03/00351	Internationales Anmeldedatum (Tag/Monat/Jahr) 21.11.2003	Prioritätsdatum (Tag/Monat/Jahr) 22.11.2002
Internationale Patentklassifikation (IPK) oder nationale Klassifikation und IPK H04L9/08		
Anmelder ARC SEIBERSDORF RESEARCH GMBH et al.		

- Dieser internationale vorläufige Prüfungsbericht wurde von der mit der internationalen vorläufigen Prüfung beauftragten Behörde erstellt und wird dem Anmelder gemäß Artikel 36 übermittelt.
- Dieser BERICHT umfaßt insgesamt 5 Blätter einschließlich dieses Deckblatts.  
  
☒ Außerdem liegen dem Bericht ANLAGEN bei; dabei handelt es sich um Blätter mit Beschreibungen, Ansprüchen und/oder Zeichnungen, die geändert wurden und diesem Bericht zugrunde liegen, und/oder Blätter mit vor dieser Behörde vorgenommenen Berichtigungen (siehe Regel 70.16 und Abschnitt 607 der Verwaltungsrichtlinien zum PCT).

Diese Anlagen umfassen insgesamt 2 Blätter.

- Dieser Bericht enthält Angaben zu folgenden Punkten:

- I ☒ Grundlage des Bescheids
- II ☐ Priorität
- III ☐ Keine Erstellung eines Gutachtens über Neuheit, erfinderische Tätigkeit und gewerbliche Anwendbarkeit
- IV ☐ Mangelnde Einheitlichkeit der Erfindung
- V ☒ Begründete Feststellung nach Regel 66.2 a)ii) hinsichtlich der Neuheit, der erfinderischen Tätigkeit und der gewerblichen Anwendbarkeit; Unterlagen und Erklärungen zur Stützung dieser Feststellung
- VI ☐ Bestimmte angeführte Unterlagen
- VII ☐ Bestimmte Mängel der internationalen Anmeldung
- VIII ☐ Bestimmte Bemerkungen zur internationalen Anmeldung

Datum der Einreichung des Antrags  16.06.2004	Datum der Fertigstellung dieses Berichts  16.12.2004
Name und Postanschrift der mit der internationalen Prüfung beauftragten Behörde   Europäisches Patentamt - P.B. 5818 Patentlaan 2 NL-2280 HV Rijswijk - Pays Bas Tel. +31 70 340 - 2040 Tx: 31 651 epo nl Fax: +31 70 340 - 3016	Bevollmächtigter Bediensteter  Liebhardt, I  Tel. +31 70 340-4114 

Zu Punkt V

**Begründete Feststellung hinsichtlich der Neuheit, der erfinderischen Tätigkeit und der gewerblichen Anwendbarkeit; Unterlagen und Erklärungen zur Stützung dieser Feststellung**

Es wird auf das folgende Dokument verwiesen:

D1: ELLIOTT C: "Building the quantum network" NEW JOURNAL OF PHYSICS, 2002, DEUTSCHE PHYSIKALISCHE GESELLSCHAFT & IOP PUBLISHING LTD, UK, Bd. 4, 12. Juli 2002 (2002-07-12), Seiten 46.1-46.12, XP002271991 ISSN: 1367-2630

1. Das Dokument D1 wird als nächstliegender Stand der Technik gegenüber dem Gegenstand des Anspruchs 1 angesehen. Es offenbart ein Kommunikationssystem mit Quantenkryptographie (Seite 46.8, Zeilen 15-26), mit an Quantenkanälen angeschlossenen *Endvermittlungsstationen* (Fig. 5, "QKD Endpoint") und den Quantenkanälen zugeordneten quantenkryptographischen Einrichtungen zur Generierung eines Quanten-Schlüssels (Seite 46.9, Zeilen 5 und 6), und mit mehreren miteinander verbundenen Vermittlungsstationen (Fig. 5, "Trusted Relay") wobei die Vermittlungsstationen über öffentliche Leitungen unter Anwendung von vereinbarter Verschlüsselung miteinander kommunizieren (Fig. 5, obere, weiße Pfeile und Seite 46.9, Zeilen 20-24), und daß die *Endvermittlungsstationen* ihrerseits mit den Vermittlungsstationen über die Quantenkanäle zur Generierung eines jeweiligen temporären Quanten-Schlüssels verbunden, und weiters zur Kommunikation über öffentliche Leitungen unter Verwendung des über die Vermittlungsstationen generierten Quanten-Schlüssels eingerichtet sind (Seite 46.9, Zeilen 20-24).
- 1.1. Der Gegenstand des Anspruchs 1 unterscheidet sich daher von dem bekannten Kommunikationssystem dadurch, daß die *Teilnehmerstationen direkt* an die Quantenkanäle angeschlossen sind und dadurch, daß die Vermittlungsstationen untereinander über öffentliche Leitungen unter Anwendung von vereinbarter Verschlüsselung *ohne quantenkryptographischen Schlüsselaustausch* kommunizieren.

Der Gegenstand des Anspruchs 1 ist somit neu (Artikel 33(2) PCT).

- 1.2. Die mit der vorliegenden Erfindung zu lösende Aufgabe kann somit darin gesehen werden, daß zum einen die durch die Quantenkryptographie gewährleistete hohe Sicherheit bis zum Endbenutzer hin erstreckt und zum anderen das Gesamtsystem durch die Verminderung der Anzahl von Vermittlungsstationen ökonomischer gestaltet werden soll.

Die in Anspruch 1 der vorliegenden Anmeldung für diese Aufgabe vorgeschlagene Lösung beruht aus den folgenden Gründen auf einer erfinderischen Tätigkeit (Artikel 33(3) PCT):

Die Aufgabenstellung der Erstreckung der besonders sicheren Quantenkryptographie bis hin zu den Endbenutzern findet im Dokument D1 keine Erwähnung. Zwar wird die Aufwendigkeit der Vermittlungsstationen in D1 angesprochen; es gibt jedoch keinen Hinweis auf die ökonomischere Gestaltung des Gesamtsystems durch die Ausführung der Kommunikation der Vermittlungsstationen untereinander über öffentliche Leitungen unter Anwendung von vereinbarter Verschlüsselung ohne quantenkryptographischen Schlüsselaustausch.

2. Die Ansprüche 2-10 sind vom Anspruch 1 abhängig und erfüllen damit ebenfalls die Erfordernisse des PCT in bezug auf Neuheit und erfinderische Tätigkeit.



**I. Grundlage des Berichts**

1. Hinsichtlich der **Bestandteile** der internationalen Anmeldung (*Ersatzblätter, die dem Anmeldeamt auf eine Aufforderung nach Artikel 14 hin vorgelegt wurden, gelten im Rahmen dieses Berichts als "ursprünglich eingereicht" und sind ihm nicht beigelegt, weil sie keine Änderungen enthalten (Regeln 70.16 und 70.17)*):

**Beschreibung, Seiten**

1-24 in der ursprünglich eingereichten Fassung

**Ansprüche, Nr.**

6 (Teil), 7-10 eingegangen am 19.06.2004 mit Schreiben vom 16.06.2004

1-5, 6 (Teil) eingegangen am 11.11.2004 mit Schreiben vom 09.11.2004

**Zeichnungen, Blätter**

1/11-11/11 in der ursprünglich eingereichten Fassung

2. Hinsichtlich der **Sprache**: Alle vorstehend genannten Bestandteile standen der Behörde in der Sprache, in der die internationale Anmeldung eingereicht worden ist, zur Verfügung oder wurden in dieser eingereicht, sofern unter diesem Punkt nichts anderes angegeben ist.

Die Bestandteile standen der Behörde in der Sprache: zur Verfügung bzw. wurden in dieser Sprache eingereicht; dabei handelt es sich um:

- ☐ die Sprache der Übersetzung, die für die Zwecke der internationalen Recherche eingereicht worden ist (nach Regel 23.1(b)).
- ☐ die Veröffentlichungssprache der internationalen Anmeldung (nach Regel 48.3(b)).
- ☐ die Sprache der Übersetzung, die für die Zwecke der internationalen vorläufigen Prüfung eingereicht worden ist (nach Regel 55.2 und/oder 55.3).

3. Hinsichtlich der in der internationalen Anmeldung offenbarten **Nucleotid- und/oder Aminosäuresequenz** ist die internationale vorläufige Prüfung auf der Grundlage des Sequenzprotokolls durchgeführt worden, das:

- ☐ in der internationalen Anmeldung in schriftlicher Form enthalten ist.
- ☐ zusammen mit der internationalen Anmeldung in computerlesbarer Form eingereicht worden ist.
- ☐ bei der Behörde nachträglich in schriftlicher Form eingereicht worden ist.
- ☐ bei der Behörde nachträglich in computerlesbarer Form eingereicht worden ist.
- ☐ Die Erklärung, daß das nachträglich eingereichte schriftliche Sequenzprotokoll nicht über den Offenbarungsgehalt der internationalen Anmeldung im Anmeldezeitpunkt hinausgeht, wurde vorgelegt.
- ☐ Die Erklärung, daß die in computerlesbarer Form erfassten Informationen dem schriftlichen Sequenzprotokoll entsprechen, wurde vorgelegt.

4. Aufgrund der Änderungen sind folgende Unterlagen fortgefallen:

- ☐ Beschreibung,      Seiten:
- ☐ Ansprüche,      Nr.:
- ☐ Zeichnungen,      Blatt:

# INTERNATIONALER VORLÄUFIGER PRÜFUNGSBERICHT

Internationales Aktenzeichen PCT/AT 03/00351

5. ☐ Dieser Bericht ist ohne Berücksichtigung (von einigen) der Änderungen erstellt worden, da diese aus den angegebenen Gründen nach Auffassung der Behörde über den Offenbarungsgehalt in der ursprünglich eingereichten Fassung hinausgehen (Regel 70.2(c)).

*(Auf Ersatzblätter, die solche Änderungen enthalten, ist unter Punkt 1 hinzuweisen; sie sind diesem Bericht beizufügen.)*

6. Etwaige zusätzliche Bemerkungen:

## V. Begründete Feststellung nach Artikel 35(2) hinsichtlich der Neuheit, der erfinderischen Tätigkeit und der gewerblichen Anwendbarkeit; Unterlagen und Erklärungen zur Stützung dieser Feststellung

1. Feststellung
- |                                |                     |
|--------------------------------|---------------------|
| Neuheit (N)                    | Ja: Ansprüche 1-10  |
|                                | Nein: Ansprüche     |
| Erfinderische Tätigkeit (IS)   | Ja: Ansprüche 1-10  |
|                                | Nein: Ansprüche     |
| Gewerbliche Anwendbarkeit (IA) | Ja: Ansprüche: 1-10 |
|                                | Nein: Ansprüche:    |

2. Unterlagen und Erklärungen:

**siehe Beiblatt**